IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,

v. 21-CR-07-V

JOHN STUART,

Defendant.

GOVERNMENT'S RESPONSE TO
DEFENDANT'S SUPPLEMENTAL BRIEFING

During oral argument on the defendant's objections to Magistrate Judge McCarthy's Report and Recommendation ("R&R") on October 13, 2023, the Court requested further briefing on two discrete issues: (1) whether a defendant has a reasonable expectation of privacy in his Internet Protocol ("IP") address such that a search could give rise to Fourth Amendment protection; and (2) whether a warrant unknowingly obtained using information collected in violation of the Fourth Amendment may nonetheless by saved by the good faith exception.

The defendant filed a supplemental brief addressing these issues, *see* Dkt. 112, however, the defendant also included newly obtained information that purportedly supports his argument that a "joint venture" existed between the FLA and the United States government. *See id.* at 5-9. As an initial matter, the government submits that this information is improperly before the Court and should be disregarded. The Court permitted supplemental briefing on the discrete issues described above and did not give *carte blanche* for the parties to

proffer additional information that could have been included in the original motion and/or objections.

Nonetheless, without conceding the accuracy of the information provided or the inferences that the defendant asks the Court to draw from it, the government submits that nothing in the defendant's supplemental briefing contradicts the government's representations or entitles him to a factual hearing. Specifically, nothing in the newly provided documents is inconsistent with TFO Hockwater's affidavit in support of the warrant application, or the government's description of the international cooperation as a "series of one-way streets" in which information is shared between the U.S. and various FLAs, but no direction is given or direct participation offered. Again, the U.S. did not direct foreign law enforcement activity, and no FLA acted on behalf of the U.S. such that it and the FLA could be said to have a "joint venture." Nothing in the defendant's supplemental memorandum suggests otherwise. The government respectfully directs the Court to its prior briefing on this issue and incorporates the same herein. *See* Dkts. 66, 87, 92, 105.

ARGUMENT

A. The defendant does not have a reasonable expectation of privacy in his IP address, even while using Tor.

In its original briefing and at oral argument, the government asserted that the defendant does not have a reasonable expectation of privacy in his IP address. *See* Dkt. 105 at 20. At oral argument, the defendant asserted that he did, in fact, have a reasonable expectation of privacy in his IP address, and requested an opportunity to submit further briefing on that point.

As the Court is well-aware, whether a defendant has a reasonable expectation of privacy in a place or thing to be searched is a two-part test. First, the defendant must have demonstrated an actual or subjective expectation of privacy; second, even if a person subjectively expected privacy, that expectation must be one that society is prepared to accept as reasonable. *See Katz v. United States*, 389 U.S. 347, 361 (1967); *California v. Greenwood*, 486 U.S. 35, 39 (1988) (holding that a defendant "must show that his subjective expectation of privacy is one that society is prepared to accept as *objectively* reasonable"). For this reason, courts routinely hold that a person does not have a reasonable expectation of privacy in information that they voluntarily disclose to third parties. *See, e.g., Smith v. Maryland*, 442 U.S. 735, 742 (1979) (holding that a person does not have a reasonable expectation of privacy in the telephone numbers he or she calls because those numbers are voluntarily disclosed to the telephone company); *United States v. Miller*, 425 U.S. 435, 443 (1976) (finding no expectation of privacy in checks and other bank records that are voluntarily disclosed to the bank).

Consistent with this longstanding principle, courts around the country have found that a person does not have a reasonable expectation of privacy in his or her IP address. *See, e.g., United States v. Christie*, 624 F.3d 558, 574 (3d Cir. 2010) (holding that a person has "no reasonable expectation of privacy in his IP address and so cannot establish a Fourth Amendment violation," due, in part, to the fact that an IP address is conveyed to and from third parties). This is true even where the internet user has used Tor in an effort to remain anonymous. *See United States v. Scanlon*, 2017 WL 3974031, *11 (D. Vt. 2017) ("any expectation by a Playpen user that his or her identity could not and would not be revealed while accessing child pornography on a publicly available website is not one society would

deem reasonable"), *aff'd on other grounds*, 774 Fed. App'x 43 (2d Cir. 2019); *United States v. Werdene*, 188 F.Supp.3d 431, 444 (E.D. Pa. 2016) ("[e]ven if Werdene maintained a subjective expectation that his IP address would remain private through his use of Tor, that expectation is not 'one that society is prepared to recognize as 'reasonable'"), *aff'd on other grounds*, 883 F.3d 204 (3d Cir. 2018); *United States v. Matish*, 193 F.Supp.3d 585, 615-18 (E.D. Va. 2016) (holding that a Tor user does not have a reasonable expectation of privacy in his or her IP address); *United States v. Michaud*, 2016 WL 337263 *6-7, Case No. 3:15-cr-05351-RJB (W.D. Wa. 2016) (same); *United States v. Adams*, 2016 WL 4212079 *3-4, Case No. 6:16-cr-11-Orl-40GJK (M.D. Fl. 2016) (same). In fact, the defendant concedes that "courts mostly agree that a typical internet user does not have a reasonable expectation of privacy in his or her IP address." Dkt. 112 at 2.

Because the extant case law is largely uniform and against him, the defendant asks this Court to extend the Supreme Court's decision in *Carpenter v. United States* beyond its narrow holding. 138 S. Ct. 2206 (2018). He argues that a Tor user's IP address is analogous to CSLI that is automatically generated any time a person interacts with a cell phone and asks the Court to diverge from nearly every other District Court to examine the issue. The Court should not do so.

First, the considerations that animated the *Carpenter* Court are not present here. The Court described the question before it in *Carpenter* as "whether the government conducts a search under the Fourth Amendment when it accesses historical cell phone records that provide a *comprehensive chronicle of the user's past movements*." *Id.* at 2211 (emphasis added). The Court was concerned with the Fourth Amendment implications of collecting information

that was "detailed, encyclopedic, and effortlessly compiled." That is because CSLI is automatically compiled by service carriers any time a cell phone user interacts with his phone in any way—even if that CSLI is in no way relevant to what the person is using the cell phone to do, *i.e.* when the user has no reason to consciously know his CSLI is being collected and recorded.

But an internet user's IP address is fundamentally different—even if the person is using Tor. A person who visits a webpage knows that his IP address is being shared with a third-party because his IP address is necessary to effectuate the visit. Even when using Tor, the user relays his true IP address to at least the entry node—and he or she knows it. *See Matish*, 193 F.Supp.3d at 616-617 ("when a user connects to the Tor network, he or she must disclose his or her real IP address to the first Tor node with which he or she connects. This fact, coupled with the Tor Project's own warning that the first server can see "[t]his IP address is using Tor," destroys any expectation of privacy in a Tor user's IP address"). Because of this, IP addresses are much more analogous to the dialing information seen in *Smith* than the CSLI at issue in *Carpenter.* This can be demonstrated by analogy.

Imagine a person—Person A—wants to discuss something nefarious with Person Z. To avoid having his telephone number identified, or the fact that he called Person Z known, he utilizes a series of relayed calls to mask his telephone number. Person A calls Person B. Person B uses a second phone, calls Person C, puts both phones on speaker, and lays them next to each other so Person A and Person C are now connected. Person C then uses a second phone and does the same with Person D. Person D does the same with Person E. And so on until Persons A and Z are able to communicate. No one in the relay outside of Person B

would know the telephone number that Person A originally called from. No one aside from Person Y would know that Person Z is the end recipient of the call. Nevertheless, no one would argue that Person A has a reasonable expectation of privacy in his phone number because he disclosed that information to both his phone carrier and at least one person is the relay—a well-reasoned conclusion consistent with a half-century of case law. *See Smith*, 442 U.S. at 742.

However, by the defendant's logic, Person A—who would have no expectation of privacy in his phone number or dialing information if he simply called Person Z directly—would suddenly have a reasonable expectation of privacy in his telephone number and call activity simply because telephone use is fairly ubiquitous in the modern world, and he took steps to mask the information from others. That conclusion finds no support in case law—and certainly finds no support in *Carpenter*.[1]

Nor should the Court rely on *United States v. Taylor*, 935 F.3d 1279, 1284 n.4 (11th Cir. 2019). The *Taylor* court did not examine the question here: whether a Tor user retains a reasonable expectation of privacy in his or her IP address. Instead, the *Taylor* decision focused on whether a Magistrate Judge in Virginia had authority to authorize a search technique that would result in the search of computers outside of that District, and, if not, whether the good faith exception applied. In its decision, the Court simply assumed, without analysis, in a single footnote that the use of Tor "t[ook] th[e] case out of third-party-doctrine land." *Id.*

[1] The government also notes that *Carpenter* was decided by a 5-4 margin and generated four separate dissenting opinions. It was therefore far from a clear-cut decision, even on its narrow facts. Although no less authoritative, the government submits that the Court should hesitate to extend *Carpenter* where, as here, the question at issue is not sufficiently analogous to clearly warrant the extension.

However, the *Taylor* court did not grapple with the third-party doctrine and its applicability to Tor use. For example, it did not explain why a Tor user's disclosure of his or her IP address to the entry node—the first Tor user in the complex relay designed to obfuscate the user's identify—does not itself put the case on all fours with *Smith* and *Miller.* The Court simply assumed that a Tor user's attempt at anonymity was enough to confer a reasonable expectation of privacy. Additionally, the *Taylor* court did not address whether such an expectation of privacy, even if subjectively held, is one that society is prepared to accept as reasonable. *See* In the absence of rigorous analysis, and against the weight of the case law, the Court should not adopt the Eleventh Circuit's assumption.

In sum, the weight of case law in this area holds that a Tor user has no reasonable expectation of privacy in his or her IP address. Nothing offered by the defendant is sufficient to overcome that well-reasoned and nearly ubiquitous conclusion. The Court should decline to extend *Carpenter* beyond its narrow facts or adopt the unreasoned assumptions of the Eleventh Circuit in *Taylor.* The Court should follow *Smith* and *Miller* and find that the defendant did not have a reasonable expectation of privacy in his IP address.

B. At all times, TFO Hockwater acted in good faith and objectively relied on the search warrant, and the good faith exception therefore applies.

The exclusionary rule is a judicially-created remedy "designed to safeguard Fourth Amendment rights generally through its deterrent effect[.]" *United States v. Calandra*, 414 U.S. 338, 348 (1974). It is not a "personal constitutional right of [a] party aggrieved." *Id.* Because of this, courts "have consistently recognized that unbending application of the exclusionary sanction to enforce ideals of governmental rectitude would impede unacceptably the truth-

finding functions of judge and jury." *United States v. Payner*, 447 U.S. 727, 734 (1980). Thus, "when law enforcement officers have acted in objective good faith or their transgressions have been minor, the magnitude of the benefit conferred on . . . guilty defendants offends basic concepts of the criminal justice system" and the Court must "weigh[] the costs and benefits of preventing the use in the prosecution's case in chief of inherently trustworthy tangible evidence obtained in reliance on a search warrant issued by a detached and neutral magistrate that ultimately is found to be defective." *United States v. Leon*, 468 U.S. 897, 907 (1984). Because of this, courts often refuse to apply the exclusionary rule where doing so is unlikely to meaningfully deter police misconduct. *Arizona v. Evans*, 514 U.S. 1, 10-11 (1995) ("the rule's application has been restricted to those instances where its remedial objectives are thought most efficaciously served. . . . Where the exclusionary rule does not result in appreciable deterrence, then, clearly, its use . . . is unwarranted.") (citations and internal quotation marks omitted).

Here, the government reiterates that there is no evidence in the record to even suggest that a Fourth Amendment violation occurred before TFO Hockwater applied for the search warrant at issue. Nevertheless, the Court has asked for additional briefing on the question of whether the Court could still apply the good faith exception assuming, *arguendo*, that a Fourth Amendment violation occurred in the identification of the defendant's IP address but was unknown to TFO Hockwater at the time he applied for the warrant.

As an initial matter, good faith will not ordinarily operate to save a search warrant where the probable cause underlying the warrant was obtained illegally by law enforcement.

In other words, an officer may not knowingly engage in an illegal search and then use the evidence obtained to apply for a subsequent warrant.

Nonetheless, that is not to say that a valid warrant may *naver* be obtained based on probable cause resulting from an illegal search. The Second Circuit's most comprehensive analysis of the issue was *United States v. Reilly*, 76 F.3d 1271 (2d Cir. 1996). In that case, two police officers unlawfully searched the curtilage of the defendant's home, deduced that he was manufacturing marijuana, and then applied for a warrant to search the property based on that information. *Id.* at 1273-75. In the application, the officers omitted crucial details about the defendant's property and the manner in which they obtained the information they had. *Id.* at 1280-82. The Second Circuit ultimately suppressed the fruits of the search. *Id.* at 1280-83. However, the Second Circuit was careful to note that it "d[id] not hold that the fruit of illegal searches can *never* be the basis for a search warrant that the police can subsequently use in good faith." *Id.* at 1280-81 (emphasis added); *see also United States v. Ganias*, 824 F.3d 199, 223 (2d Cir. 2016) ("it is not the case that good faith reliance on a warrant is never possible in circumstances in which a predicate constitutional violation has occurred."). In drawing that distinction, the Court placed great emphasis on the fact that it was the officers themselves that (a) were responsible for the illegally obtained evidence, and (b) knowingly failed to disclose pertinent aspects of the investigation to the magistrate. *Id.* In essence, they were not truly acting in "good faith," and their reliance on a warrant was not objectively reasonable, such that the good faith exception would apply.

This stands in sharp contrast to the hypothetical posed here because there is no question that TFO Hockwater acted in good faith when he obtained and executed the warrant.

TFO Hockwater accurately relayed information that was given to him by other law enforcement personnel who were removed from the investigation of the defendant and whom he had no reason not to trust. Any information withheld by those other actors should not then be held against TFO Hockwater who accurately represented the information provided to him in a good faith effort to obtain a search warrant—in other words, TFO Hockwater did not engage in any misconduct that exclusion would deter. *See United States v. Raymonda*, 780 F.3d 105, 118 (2d Cir. 2015) ("When an officer genuinely believes that he has obtained a valid warrant from a magistrate and executes the warrant in good faith, there is no conscious violation of the Fourth Amendment, and thus nothing to deter by suppression) (citations and internal quotation marks omitted). This is especially true where TFO Hockwater was not the law enforcement officer who engaged in the hypothetical antecedent violation.[2] *See United States v. McClain*, 444 F.3d 556, 566 (6th Cir. 2005) ("Because the officers who sought and executed the search warrants acted with good faith, and because the facts surrounding the initial warrantless search were close enough to the line of validity to make the executing officers' belief in the validity of the search warrants objectively reasonable, we conclude that despite the initial Fourth Amendment violation, the *Leon* exception bars application of the exclusionary rule in this case").[3]

[2] Most of the case law identified by the government involves situations in which the same officer who committed the Fourth Amendment violation then applied for a warrant using it. In such a case, excluding evidence makes sense because the person who obtained the warrant is the very person to be deterred by the exclusionary rule. However, that is fundamentally different than the hypothetical here, in which TFO Hockwater and the local investigation team were not a party to any Fourth Amendment violation. Under these circumstances, excluding evidence would not have a deterrent effect on TFO Hockwater, and would be unlikely to have a deterrent effect on an FLA or some far-off law enforcement personnel who are not actively involved in the investigation of the defendant. *See, e.g, United States v. Lee*, 723 F.3d 134, 139-140 (2d Cir. 2013) (noting that the exclusionary rule is not typically applied to misconduct by foreign law enforcement or private actors because it would be unlikely to have a deterrent effect).

[3] The *McClain* court outlined a potential Circuit split in this area of the law. *See McClain*, 444 F.3d at 564-566.

In sum, although an antecedent Fourth Amendment violation will ordinarily preclude reliance on a subsequent warrant based on that illegally obtained evidence, the good faith exception may still apply where, as here, the officers who obtain and execute the defective warrant do so in good faith in objective reliance on the existence of the warrant. Nothing in the record suggests that TFO Hockwater was not acting in good faith when he obtained the search warrant, and his reliance on that warrant was reasonable. The Court should therefore apply the good faith exception, even if, arguendo, the FLA engaged in an unlawful search to obtain the defendant's IP address.

CONCLUSION

For all of the foregoing reasons, the Court should adopt the R&R, and deny the defendant's motions.

DATED: Buffalo, New York, December 26, 2023

TRINI E. ROSS
United States Attorney

BY: ***/s/DAVID J. RUDROFF***
Assistant United States Attorney
United States Attorney's Office
Western District of New York
138 Delaware Avenue
Buffalo, NY 14202
716/843-5806
David.Rudroff@usdoj.gov